Desain dan Implementasi Standar Operasional Prosedur (SOP) Keamanan Sistem Informasi Fakultas Teknik Universitas Diponegoro Menggunakan Standar ISO 27001

Penji Prasetya[1)], Adian Fatchur Rochim[2)], Ike Pertiwi Windasari[2)]
Program Studi Sistem Komputer Fakultas Teknik Universitas Diponegoro
Jalan Prof. Sudharto, Tembalang, Semarang, Indonesia
penjiprasetya@hotmail.com

***Abstract* - Like today's modern era, information technology is needed to support the business processes of the organization. In the use of information technology organization must have policies and standard operating procedures are good that any work carried out in the appropriate direction of the organization. Not only that, the organization must also pay attention to information security of any assets owned. This final project aims to make policies and standard operating procedures (SOP) and assessing the information security risk in the assets of the organization. In the process of this skripsi refers to the standard of ISO 27001 as the standard for information security management and use of qualitative methodology, where qualitative methodology is a methodology that produces descriptive data in the form of words written or spoken of people and behaviors that can be observed.**

This final project resulted in the level of risk that is contained in the value of assets and generate recommendations to improve the security controls in the information security of assets based on the clauses of ISO 27001. In accordance with the initial objective of this final project also produce information security policy document and document information security standard operating procedures.

***Key Terms:* information security, Standard operating procedure (SOP), ISO 27001**

I. PENDAHULUAN

SAAT sekarang ini penggunaan teknologi infomasi sangatlah diperlukan untuk mendukung proses bisnis dan menunjang kinerja organisasi. Dengan adanya teknologi informasi setiap divisi yang ada di sebuah organisasi akan terbantu dalam pengerjaan tugas-tugasnya. Dalam penggunaan teknologi informasi organisasi harus memiliki kebijakan dan standar operasional prosedur yang baik agar setiap pekerjaan yang dilakukan berjalan sesuai arahan organisasi. Tidak hanya itu organisasi juga harus memperhatikan keamanan informasi dari setiap aset-aset yang dimiliki.

Pada tahun 2008, Kementerian Komunikasi dan Informasi (Kominfo) dalam meningkatkan kesadaran akan pentingnya keamanan informasi telah menyelenggarakan sosialisasi dan bimbingan teknis kepada instansi penyelenggara pelayanan publik, baik di lingkungan pemerintah pusat maupun daerah. Dalam melakukan sosialisasi, Kementerian Kominfo menggunakan standar ISO 27001 untuk pendekatan dalam melakukan penerapan keamanan informasi. Kementerian Kominfo berharap nantinya semua instansi penyelenggara pelayanan publik memiliki dokumentasi sistem manajemen keamanan informasi yang memenuhi standar ISO 27001. (Kemkominfo, 2011).

Sebelumnya sudah ada sebuah penelitian mengenai tata kelola teknologi informasi di Fakultas Teknik Universitas Diponegoro menggunakan kerangka kerja COBIT 4.1. Penelitian dilakukan oleh saudari Arini Arumana. Berdasarkan analisis tata kelola TI di Fakultas Teknik, didapat tiga proses yang memiliki tingkat kematangan terendah, yakni proses PO6 *Communicate management aims and direction*, PO8 *Manage quality* dan ME4 *Provide IT governance*, dengan nilai kematangan 1 dan berada pada tingkat *initial / ad-hoc*, dimana kondisinya tidak ada proses yang baku. Juga beberapa kelemahan dalam proses TI yang berjalan, diantaranya penetapan dan dokumentasi tindakan, kebijakan dan prosedur yang minim.

Berdasarkan hasil penelitian tersebut dapat dilihat beberapa kelemahan dalam proses TI yang berjalan antara lain dokumentasi, kebijakan dan prosedur di fakultas teknik masih minim. Sedangkan untuk menunjang proses kerja yang baik kebijakan dan prosedur merupakan faktor pendukung dalam menciptakan proses kerja yang baik agar sesuai rencana dan arahan organisasi. Sehubungan dengan ini diperlukan adanya pembuatan standar operasional prosedur (SOP) untuk mengatur dan membuat proses TI di Fakultas Teknik lebih terstruktur, juga meningkatkan kualitas keamanan dalam pengelolaan sistem informasi di Fakultas Teknik.

Tujuan dari tugas akhir ini adalah membuat kebijakan dan standar operasional prosedur mengenai keamanan sistem informasi fakultas teknik menggunakan standar ISO 27001.

II. DASAR TEORI

A. Keamanan Informasi

Keamanan Informasi adalah penjagaan informasi dari seluruh ancaman yang mungkin terjadi dalam upaya untuk memastikan atau menjamin kelangsungan bisnis (*business continuity*), meminimasi risiko bisnis (*reduce business risk*) dan memaksimalkan atau mempercepat pengembalian investasi dan peluang bisnis (ISO 27001 dalam Sarno dan Iffano, 2009).

B. *Aspek Keamanan Informasi*

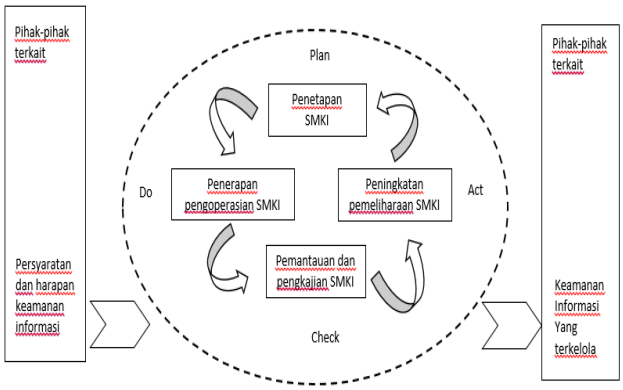
Dalam merancang sistem keamanan informasi yang baik, ada aspek-aspek keamanan informasi yang harus di perhatikan. Aspek-aspek tersebut antara lain:

1) *Confidentiality*
   Harus menjamin bahwa yang bisa mengakses informasi tertentu hanyalah mereka yang mempunyai hak.
2) *Integrity*
   Harus menjamin kelengkapan informasi dan menjaga dari kerusakan atau ancaman lain yang bisa menyebabkan perubahan pada informasi asli.
3) *Availability*
   Harus menjamin pengguna dapat mengakses informasi tanpa adanya gangguan dan tidak dalam format yang tidak bisa digunakan. Pengguna dalam hal ini bisa berarti manusia atau sistem yang mempunyai hak untuk mengakses informasi tersebut. (Peltier, T. R., 2001)

C. *ISO 27001*

ISO/IEC 27001:2005 merupakan standar keamanan informasi yang menggantikan BS-7799:2 dan diterbitkan pada bulan Oktober 2005 oleh *International Organization for Standarization* dan *International Electrotechnical Commission.* (Calder, Alan., Steve Watkins. 2008).

Standar ini mengadopsi "Plan-Do-Check-Act" (PDCA) model, yang digunakan untuk mengatur semua proses SMKI. Standar ini juga memberikan model untuk menerapkan prinsip-prinsip dalam pedoman yang mengatur penilaian risiko, desain keamanan dan implementasi, manajemen keamanan dan penilaian ulang. (SNI ISO/IEC 27001:2009). keseluruhan proses SMKI dapat dipetakan seperti pada Gambar 1 berikut.



Gambar 1. Model PDCA yang diterapkan untuk proses SMKI (Sumber :SNI ISO/IEC 27001:2009)

ISO 27001 memiliki 11 klausul kontrol keamanan (*security control*), 39 objektif control (*control objectives*) dan 133 kontrol keamanan/control (*controls*). 11 klausul kontrol keamanannya adalah sebagai berikut:

1) Kebijakan keamanan informasi
2) Organisasi keamanan informasi
3) Manajemen aset
4) Sumber daya manusia menyangkut keamanan informasi
5) Keamanan fisik dan lingkungan
6) Komunikasi dan manajemen operasi
7) Akses control
8) Pengadaan/akuisisi, pengembangan dan pemeliharaan sistem informasi
9) Pengelolaan insiden keamanan informasi
10) Manajemen kelangsungan usaha (*business continuity management*)
11) Kepatuhan (Kemkominfo, 2011)

D. *Standar Operasional Prosedur (SOP)*

Pengertian standar operasional prosedur (SOP) menurut Istyadi Insani, dalam bukunya yang berjudul standar operasional prosedur (SOP) sebagai pedoman pelaksanaan administrasi perkantoran dalam rangka peningkatan pelayanan dan kinerja organisasi pemerintah menyatakan bahwa "SOP adalah dokumen yang berisi serangkaian instruksi tertulis yang dibakukan mengenai berbagai proses penyelenggaraan administrasi perkantoran yang berisi cara melakukan pekerjaan, waktu pelaksanaan, tempat penyelenggaraan dan aktor yang berperan dalam kegiatan."(Insani, Istyadi, 2010).

III. METODOLOGI PENELITIAN

A. *Metodologi Penelitian*

Pada bagian ini akan membahas mengenai metodologi penelitian. Metodologi penelitian yang digunakan adalah jenis penelitian *kualitatif* dengan pendekatan *deskriptif*. Penelitian *kualitatif* didefinisikan oleh Bogdan & Taylor (1975) dalam Moleong (2006) adalah sebagai prosedur penelitian yang menghasilkan data *deskriptif* berupa kata-kata tertulis atau lisan dari orang-orang dan perilaku yang dapat diamati.

B. *Tahapan Penelitian*

Gambar 2. Tahapan Penelitian

1) Tahapan Perencanaan
   Tahapan perencanaan merupakan tahapan awal dari penelitian. Tahap ini masih dalam tahap studi pustaka, perumusan latar belakang, perumusan masalah serta pembatasan masalah dari penelitian. Studi pustaka yang dilakukan yaitu mempelajari referensi-referensi penelitian dari jurnal, e-book, buku serta konsultasi dengan dosen pembimbing terkait penelitian yang dilakukan. Studi pustaka yang dimaksud meliputi sistem manajemen keamanan informasi dari ISO 27001, metode manajemen risiko, standar operasional prosedur serta bagaimana mengelola keamanan informasi yang baik berdasarkan ISO 27001 sebagai kerangka kerja utama dalam penelitian ini.
2) Tahapan Persiapan
   Dalam tahapan ini penelitian mulai masuk kedalam bagian penentuan ruang lingkup dan pemetaan organisasi sebagai objek dari penelitian. Berdasarkan panduan penerapan tata kelola keamanan informasi yang dibuat oleh kemkominfo penentuan ruang lingkup yang dilakukan meliputi:
   1) Proses dan Kegiatan. Misalnya: Melakukan identifikasi aset informasi yang dimiliki organisasi, melakukan

analisa risiko aset dan melakukan desain dan implementasi standar operasional prosedur keamanan sistem informasi.

2) Satuan Kerja : Sistem Informasi Fakultas Teknik
3) Lokasi kerja : Fakultas Teknik Universitas Diponegoro

3) Tahapan Pelaksanaan

Tahapan pelaksanaan merupakan tahapan inti dalam penelitian ini, dimana dalam tahapan pelaksanaan semua proses-proses penelitian sudah dilakukan seperti identifikasi aset, analisa risiko, serta penilaian risiko pada aset. Proses identifikasi aset merupakan proses pengidentifikasian pada aset-aset yang dimiliki oleh unit sistem informasi fakultas teknik. Untuk melakukan identifikasi aset diperlukan survei ke unit sistem informasi fakutas teknik serta melakukan observasi dan wawancara kepada pihak terkait dari penelitian. Aset yang diidentifikasi terdiri dari 6 kategori aset yaitu : aset sumber daya manusia, aset data, aset sarana pendukung, aset fasilitas, aset perangkat keras dan jaringan, serta yang terakhir aset perangkat lunak. Adapun contoh dari 6 kategori aset ditunjukkan pada Tabel I sebagai berikut.

TABEL I
CONTOH KATEGORI ASET

No	Nama aset
Aset sumber daya manusia	
1.	Pegawai tetap
Aset sarana pendukung	
2	Genset manual
Aset data	
3.	Dokumen peminjaman
Aset fasilitas	
4	Rak server
Aset perangkat keras dan jaringan	
5.	Server
Aset perangkat lunak	
6.	Sistem operasi

Setelah dilakukannya tahapan pengambilan data berupa identifikasi aset yang ada pada unit SIFT, tahap selanjutnya adalah melakukan analisa risiko, dimana dalam analisa risiko terdapat beberapa poin yang harus dianalisa seperti identifikasi risiko atau melakukan analisa kritikalitas berdasarkan *confidentiality*, *integrity* dan *availabilty*, selanjutnya melakukan analisa kecenderungan dan analisa dampak yang ada pada aset. Adapun contoh dari dari analisa risiko antara lain dapat dilihat pada Tabel II berikut.

TABEL II
CONTOH IDENTIFIKASI RISIKO (ANALISA KRITIKALITAS)

No	**Nama Aset**	**C**	**I**	**A**	**Kritikalitas**
1.	PC	H	H	H	Kritikal
2.	LCD TV	M	M	M	Tidak kritikal
3.	Printer	M	M	M	Tidak kritikal

Tabel diatas merupakan contoh dari analisa kritikalitas. Pada tabel selanjutnya merupakan contoh tabel analisa kecenderungan dan dampak dapat dilihat pada Tabel III berikut.

TABEL III
CONTOH TABEL ANALISA KECENDERUNGAN DAN DAMPAK

Aset	Deskripsi Risiko			Kontrol yang ada saat ini
	Kerawanan	Ancaman	Effect	
PC	Kurang baiknya manajemen pengamanan dan hak akses fisik ruangan	PC dapat diakses oleh pihak yang tidak berwenang	Kerahasiaan data lebih mudah diketahui oleh pihak yang tidak berwenang	-perimeter gedung (kunci dan pembatas fisik) - Penerimaan tamu gedung - petugas keamanan

4) Tahapan penerapan

Tahap penerapan merupakan tahapan terakhir dari penelitian. Ada 2 langkah yang dilakukan dalam tahapan penerapan ini yaitu : Pemetaan *Objective kontrol* & *control* serta pembuatan kebijakan dan standar operasional prosedur keamanan informasi. Dimana pembuatan kebijakan dan standar opersional prosedur ini merupakan tujuan utama dalam penelitian.

C. Metode Pengumpulan Data

Metode pengumpulan data yang digunakan dalam penelitian ini adalah proses survei, observasi, dan wawancara.

1) Survei

Proses survei digunakan untuk mendapatkan keterangan-keterangan tentang gambaran umum dari penelitian. Dimana dengan adanya informasi secara umum dari pihak yang terkait dapat memudahkan dalam melakukan proses penelitian yang berikutnya.

2) Observasi

Metode observasi adalah suatu cara untuk mengumpulkan data dengan pengamatan secara langsung kepada suatu objek yang akan diteliti. Metode observasi dilakukan dengan cara pengamatan langsung di tempat berlangsungnya penelitian, dalam hal ini penelitian dilakukan di Fakultas teknik universitas diponegoro.

3) Wawancara

Metode wawancara adalah suatu metode pengumpulan data dengan cara menanyakan atau mewawancarai secara langsung sumber-sumber terkait mengenai pembuatan dan penerapan proses standar operasional prosedur keamanan sistem informasi di Fakultas teknik.

IV. HASIL DAN PEMBAHASAN

A. Hasil Identifikasi Aset

Setelah melakukan penelitian pada unit sistem informasi fakultas teknik, maka ada 6 kategori aset yang berhasil diidentifikasi antara lain dapat dilihat pada tabel-tabel dibawah ini. Kategori aset pertama yang ditemukan dari tahapan identifikasi yaitu aset sumber daya manusia. Kategori dari aset sumber daya manusia yang terdapat di dalam unit sistem informasi fakultas teknik ditunjukkan dalam Tabel IV berikut.

TABEL IV
REGISTRASI ASET SUMBER DAYA MANUSIA (SDM)

No	**Nama Aset**
1.	Operator BAA
2.	Pegawai kontrak (Operator EDP)
3.	Pegawai tetap (Koordinator, supervisor, teknisi)

Selanjutnya aset yang didapat yaitu pada kategori aset data. Kategori dari aset data yang terdapat di dalam unit sistem informasi fakultas teknik ditunjukkan dalam Tabel V berikut.

TABEL V
REGISTRASI ASET DATA

No	Nama Aset
1.	SOP 001/2009 : penataan IP, VOIP, dan video conference
2.	SOP 001/2011 : Update status penetapan tagihan biaya kuliah
3.	SOP 005/2011 : Persetujuan dosen wali pada sistem akademik
4.	SOP 005/2009 : Standarisasi website bilingual
5.	SOP 004/2011 : Aplikasi evaluasi proses pembelajaran
6.	SOP 010/2011 : Sistem informasi kepegawaian
7.	SOP 006/2011 : Penggunaan virtual class
8.	SOP 003/2011 : Portal single sign on
9.	SOP 009/2011 : Sistem informasi eksekutif untuk grub user
10.	SOP 004/2009 : Indeksasi dan social media
11.	SOP 003/2009 : Keamanan website dan portal
12.	SOP 008/2011 : Sistem untuk grub BAK
13.	SOP 002/2011 : Her-registrasi mahasiswa
14.	SOP 007/2011 : Sistem informasi akademik untuk grub EDP
15.	Buku keluhan sistem pelayanan sistem dan jaringan
16.	Buku peminjaman inventaris
17.	SOP 002/2009 : Panduan operasional web master
18.	*Back up* CD untuk data SIA

Kategori aset selanjutnya yang didapat yaitu pada kategori aset sarana pendukung. Kategori dari aset sarana pendukung yang terdapat di dalam unit sistem informasi fakultas teknik ditunjukkan dalam Tabel VI berikut.

TABEL VI
REGISTRASI ASET SARANA PENDUKUNG

No	Nama Aset
1.	Genset manual
2.	UPS
3.	AC

Selanjutnya aset yang didapat yaitu pada kategori aset fasilitas. Kategori dari aset fasilitas yang terdapat di dalam unit sistem informasi fakultas teknik ditunjukkan dalam Tabel VII berikut.

TABEL VII
REGISTRASI ASET FASILITAS

No	Nama Aset
1.	Ruang penyimpanan server
2.	Rak server
3.	Rak aset data

Selanjutnya aset yang didapat yaitu pada kategori aset perangkat keras dan jaringan. Kategori dari aset perangkat keras dan jaringan yang terdapat di dalam unit sistem informasi fakultas teknik ditunjukkan dalam Tabel VIII berikut.

TABEL VIII
REGISTRASI ASET PERANGKAT KERAS DAN JARINGAN

No	Nama Aset
1.	PC
2.	LCD TV
3.	Printer
4.	Monitor LCD
5.	Router
6.	Switch Layer 2
7.	Switch Layer 3
8.	Akses Point
9.	Server
10.	KVM Switch

Selanjutnya aset yang didapat yaitu pada kategori aset perangkat lunak. Kategori dari aset perangkat lunak yang terdapat di dalam unit sistem informasi fakultas teknik ditunjukkan dalam Tabel IX berikut.

TABEL IX
REGISTRASI PERANGKAT LUNAK

No	Nama Aset
1.	SMS Broadcast
2.	Sistem Infomasi laboratorium
3.	Sistem Informasi Kepegawaian
4.	Evaluasi undip
5.	Sistem Informasi Billing
6.	Sistem Informasi Keuangan
7.	Single sign on
8.	e-conference
9.	Sistem informasi perpustakaan
10.	Sistem informasi dokumen
11.	Sistem informasi akademik

B. Analisa Risiko

Berdasarkan ISO 27001:2005 ISMS manajemen risiko, Tahapan analisa risiko memiliki beberapa kategori seperti identifikasi risiko atau menganalisa kritikalitas, analisa kecenderungan dan dampak dengan menggunakan kriteria kerawanan, ancaman dan dampak serta kecenderunagn risiko berdasarkan ISO 27001:2005 ISMS manajemen risiko. Analisa risiko berfungsi untuk mengetahui risiko apa saja yang dapat menyerang aset dan seberapa besar dampak dari risiko tersebut bagi aset.

C. Identifikasi Risiko

Proses identifikasi risiko digunakan sebagai acuan dasar untuk mengetahui risiko yang ada pada suatu aset. dalam identifikasi risiko digunakan cara menganalisa kritikalitas dan menghitung nilai kritikalitas pada aset tersebut. Analisa ini berguna untuk mengetahui tinggi dan rendahnya tingkat kritikalitas aset bagi organisasi.

Dari hasil analisa yang dilakukan diketahui ada 36 aset yang berada pada kategori krtitikal dan 12 aset berada pada kategori tidak kritikal. Salah satu hasil dari tahapan identifikasi risiko ditunjukkan pada Tabel X berikut.

TABEL X
SALAH SATU HASIL TAHAPAN IDENTIFIKASI RISIKO ASET PERANGKAT KERAS DAN JARINGAN

No	Nama Aset	C	I	A	Kritikalitas
1.	PC	H	H	H	Kritikal
2.	LCD TV	M	M	M	Tidak kritikal
3.	Printer	M	M	M	Tidak kritikal
4.	Monitor LCD	M	M	M	Tidak kritikal
5.	Router	H	H	H	Kritikal
6.	Switch Layer 2	H	H	H	Kritikal
7.	Switch Layer 3	H	H	H	Kritikal
8.	Akses Point	H	H	H	Kritikal
9.	Server	H	H	H	Kritikal
10.	KVM Switch	H	H	H	Kritikal

Tahap identifikasi risiko ini merupakan tahapan awal dari proses analisa risiko. Setelah melakukan identifikasi risiko berdasarkan kritikalitas pada aset selanjutnya akan dihitung nilai pada aset yang telah teridentifikasi. Penilaian yang dilakukan menggunakan rumus :

$$Asset\ Value = (Confidentiality + Integrity + Availability) / 3$$

Hasil penghitungan nilai aset berdasarkan kriteria kritikalitas ditunjukkan pada Tabel XI berikut.

TABEL XI
SALAH SATU HASIL PENGHITUNGAN NILAI ASET PERANGKAT KERAS DAN JARINGAN

No	Nama Aset	C	I	A	Nilai aset
1.	PC	3	3	3	3

2.	LCD TV	2	2	2	2
3.	Printer	2	2	2	2
4.	Monitor LCD	2	2	2	2
5.	Router	3	3	3	3
6.	Switch Layer 2	3	3	3	3
7.	Switch Layer 3	3	3	3	3
8.	Akses Point	3	3	3	3
9.	Server	3	3	3	3
10.	KVM Switch	3	3	3	3

D. Analisa Kecenderungan dan Dampak

Setelah dilakukannya tahapan identifikasi risiko berdasarkan kritikalitas pada aset dengan mengarah pada kriteria penilaian *confidentiality*, *integrity*, dan *availability*. Selanjutnya akan dilakukan analisa risiko aset berdasarkan kriteria ancaman *(Threat)*, kerawanan *(Vulnerability)* dan dampak *(Effect)*. Hasil dari analisa kecenderungan dan dampak di tunjukkan pada Tabel XII berikut:

TABEL XII
HASIL ANALISA KECENDERUNGAN DAN DAMPAK

Kategori Aset	Aset	Deskripsi Risiko			Kontrol yang ada saat ini	Risiko inheren	
		Kerawanan	Ancaman	Effect		Nilai dampak	Nilai kecenderungan
Aset Perangkat keras Dan jaringan	PC	Kurang baiknya manajemen pengamanan dan hak akses fisik ruangan	PC dapat diakses oleh pihak yang tidak berwenang	Kegiatan terkait pengadaan secara elektronik terganggu	-perimeter gedung (kunci dan pembatas fisik) - Penerimaan tamu gedung - petugas keamanan	1	1
	LCD TV	Di letakkan di tempat umum yang dapat dilihat oleh siapa saja	Rawan kehilangan	Tidak dapat memonitor jaringan dari layar LCD TV	-perimeter gedung (kunci dan pembatas fisik) - Penerimaan tamu gedung - petugas keamanan	1	1
Dan Seterusnya							

Setelah menentukan nilai kecenderungan dan nilai dampak selanjutnya dilakukan perhitungan penilaian risiko akhir. Perhitungan ini didapat dengan menggunakan rumus :

Nilai Risiko = Nilai Dampak x Nilai Kecenderungan

Setelah melakukan penghitungan nilai risiko, hasil dari penilaian tersebut akan dibagi kedalam beberapa tingkatan kategori antara lain kategori rendah, sedang dan tinggi. Masing-masing tingkatan juga akan memiliki nilai yang tersendiri antara lain :

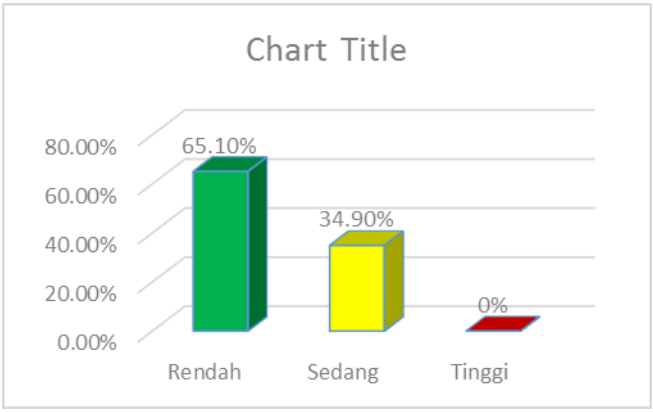
Nilai 0 - 5 : Rendah
Nilai 6 – 11: Sedang
Nilai 12 – 16 : Tinggi

Berikut ini merupakan matriks nilai risiko yang akan ditunjukkan pada Gambar 3 sebagai berikut.

Tingkat Kecenderungan \ Tingkat Dampak									
	0	1	2	3	4	5	6	7	8
	1	2	3	4	5	6	7	8	9
	2	3	4	5	6	7	8	9	10
	3	4	5	6	7	8	9	10	11
	4	5	6	7	8	9	10	11	12
	5	6	7	8	9	10	11	12	13
	6	7	8	9	10	11	12	13	14
	7	8	9	10	11	12	13	14	15
	8	9	10	11	12	13	14	15	16

Gambar 3. Matriks nilai risiko

Dari hasil penghitungan keseluruhan nilai risiko jika dilihat berdasarkan persentase persebaran risiko maka nilai risiko pada kategori rendah berjumlah 65,10 % dan pada kategori sedang berjumlah 34,90 % dan dapat dilihat pada Gambar 4 berikut.



Gambar 4. Persentase nilai risiko

E. Pemetaan Control Objective & Control

Pemetaan *control objective & control* ini berdasarkan dari ISO 27001, dimana pada masing-masing aset akan dikontrol melalui klausul-klausul yang dimiliki oleh ISO 27001 guna mengurangi risiko yang ada pada masing-masing aset. Pengontrolan ini tidak terbatas pada aset yang bernilai tinggi ataupun rendah, tetapi lebih kepada semua aset yang telah teridentifikasi di awal. Karena setiap aset yang teridentifikasi memiliki fungsi dan peran yang saling mendukung satu sama lain dalam proses kerja unit sistem informasi fakultas teknik. Maka dari itu diperlukannya pengontrolan agar mengurangi risiko yang terjadi dikemudian harinnya.

Hasil dari pemetaan *control objective & control* di tunjukkan pada Tabel XIII berikut.

TABEL XIII
PEMETAAN *CONTROL OBJECTIVE & CONTROL*

Kategori Aset	Aset	Deskripsi Risiko			Kontrol yang ada saat ini	Kontrol ISO 27001
		Kerawanan	Ancaman	Effect		
Aset Perangkat keras	PC	Kurang baiknya manajemen pengamanan dan hak akses fisik ruangan	PC dapat diakses oleh pihak yang tidak berwenang	Kegiatan terkait pengadaan secara elektronik terganggu	-perimeter gedung (kunci dan pembatas fisik) - Penerimaan tamu gedung - petugas keamanan	A.9.1 (Area yang aman) A.10.7.1 (manajemen media yang dapat dipindahkan)
	LCD TV	Di letakkan di tempat umum yang dapat dilihat oleh siapa saja	Rawan kehilangan	Tidak dapat memonitor jaringan dari layar LCD TV	-perimeter gedung (kunci dan pembatas fisik) - Penerimaan	A.9.1 (Area yang aman) A.10.7.1 (manajemen media yang dapat dipindahkan)

F. Pembuatan Kebijakan dan Standar Operasional Prosedur

Berdasarkan piramida sistem manajemen keamanan informasi, struktur dokumen sistem manajemen keamanan informasi terdiri dari 3 tingkat yaitu: pada tingkatan pertama

struktur kebijakan dan standar, pada tingkatan kedua prosedur, panduan, petunjuk dan pelaksanaan dan yang terakhir pada tingkatan ketiga struktur petunjuk teknis, instruksi kerja dan formulir. Pada penelitian ini juga akan menerapkan proses dari piramida sistem manajemen keamanan informasi, dimana tahapan awal yang akan dilakukan setelah adanya tahapan identifikasi aset, identifikasi risiko, analisa risiko, analisa kecenderungan dan dampak. Selanjutnya adalah menyusun kebijakan keamananan informasi yang sumber pembuatannya diambil dari hasil pemetaan klausul ISO 27001. Dimana kebijakan itu sebagai arahan dalam melakukan proses-proses kerja berdasarkan keamanan informasi ISO 27001. Dan setelah melakukan penyusunan kebijakan, langkah selanjutnya adalah mendesain standar operasional prosedur (SOP) yang bertujuan untuk instruksi-instruksi kerja dalam sistem manajemen keamanan informasi.

Adapun hasil dari dokumen kebijakan dan standar operasional prosedur keamanan sistem informasi ditunjukkan pada tabel-tabel berikut.

Daftar kebijakan keamanan sistem informasi ditunjukkan pada Tabel XIV berikut.

TABEL XIV
DAFTAR KEBIJAKAN KEAMANAN SISTEM INFORMASI

No	Kebijakan keamanan informasi
1	Kebijakan *Back-up*
2	Kebijakan manajemen password pengguna
3	Kebijakan keamanan area yang aman
4	Kebijakan penanganan media
5	Kebijakan operasional fasilitas pengolahan informasi
6	Kebijakan mengelola keamanan informasi
7	Kebijakan akses kontrol
8	Kebijakan pengelolaan aset
9	Kebijakan keamanan sumber daya manusia

Daftar standar operasional prosedur keamanan sistem informasi ditunjukkan pada Tabel XV berikut.

TABEL XV
DAFTAR STANDAR OPERASIONAL PROSEDUR KEAMANAN SISTEM INFORMASI

No	Standar operasional prosedur keamanan informasi
1	Prosedur *Back-up* dokumen
2	Prosedur CD/DVD
3	Prosedur pemeliharan rutin
4	Prosedur perbaikan aset
5	Prosedur keamanan sumber daya manusia setelah bekerja
6	Prosedur keamanan sumber daya manusia Pengakhiran pekerjaan
7	Prosedur manajemen insiden keamanan informasi terhadap serangan hacker
8	Prosedur manajemen keamanan insiden keamanan informasi terhadap virus atau program jahat
9	Prosedur manajemen insiden keamanan informasi pad fasilitas informasi
10	Prosedur pengendalian instalasi perangkat lunak
11	Prosedur pengendalian perubahan perangkat lunak
12	Prosedur pemeliharaan peralatan dan sarana pendukung
13	Prosedur pengendalian jaringan

V. KESIMPULAN DAN SARAN

Pada bagian ini akan dijelaskan kesimpulan dan saran dari hasil penelitian dan pembahasan.

A. Kesimpulan

Berdasarkan hasil penelitian yang dilakukan dalam *desain* dan implementasi standar operasional prosedur (SOP) keamanan informasi menggunakan ISO/IEC 27001:2005, maka dapat disimpulkan hal-hal sebagai berikut :

1) Berdasarkan hasil analisa kritikalitas aset yang mengacu pada kriteria kerahasiaan (*confidentialty*), keutuhan (*integrity*), dan ketersediaan (*availability)*, dari seluruh aset yang diidentifikasi terdapat 36 aset memiliki tingkat kritikalitas pada kategori "kritikal" dan 12 aset pada kategori "tidak kritikal".
2) Berdasarkan hasil analisa risiko yang mengacu pada ISMS ISO 27001 manajemen risiko, didapat pada aset data memiliki level risiko yang lebih tinggi yaitu pada kategori "sedang", dibandingkan aset-aset yang lain seperti aset perangkat keras, aset perangkat lunak, aset fasilitas, aset sarana pendukung, dan aset sumber daya manusia. Karena celah keamanan dari aset data sendiri masih sangat terbuka dan masih mudah diakses oleh pihak umum. Maka sekiranya perlu adanya sebuah kebijakan pengamanan dan prosedur pemeliharaan media serta kebijakan lain untuk meningkatkan keamanan dari aset tersebut.
3) Berdasarkan hasil penelitian keamanan informasi yang menyesuaikan dari hasil identifikasi dan analisa risiko pada aset, maka dapat tersusun 2 dokumen keamanan informasi yang terdiri dari 9 kebijakan keamanan informasi dan 13 standar operasional prosedur (SOP) keamanan informasi.

B. Saran

Saran yang dapat diberikan oleh penulis adalah sebagai berikut :

1) Disarankan bagi peneliti untuk proses pengidentifikasi dokumen-dokumen yang dibutuhkan hendaknya dibahas lebih mendetail dengan diskusi dengan pihak-pihak terkait sehingga dapat lebih mengerti proses manajemen keamanan informasi dari tempat penelitian.
2) Dalam penelitian ini hanya berfokus pada standar keamanan informasi ISO/IEC 27001:2005. Diharapkan dalam penelitian berikutnya disertakan juga perbandingan manajemen keamanan informasi antara ISO, COBIT dan standar keamanan informasi yang lain agar hasil lebih optimal

DAFTAR PUSTAKA

[1] Arini Arumana., Analisis Tata Kelola Teknologi Informasi Menggunakan Kerangka Kerja Cobit 4.1 Pada Fakultas Teknik Universitas Diponegoro, Skripsi S-1, Universitas Diponegoro, Semarang, 2014.

[2] Calder, Alan, Steve Watkins. 2008. IT Governance – A Managers Guide to Data Securiy And ISO 27001 – ISO 27002.

[3] ISO/IEC 27001:2005, Information technology – Security techniques – Information security management systems – Requirements.

[4] ISO/IEC 27001: 2005 , *ISMS* manajemen risiko

[5] ISO/IEC 27005: 2008 , *Information technology – Security techniques – Information security risk management.s*

[6] Insani, Istyadi. 2010. *Standar Operasional Prosedur (SOP) Sebagai Pedoman Pelaksanaan Administrasi Perkantoran Dalam Rangka Peningkatan Pelayanan Dan Kinerja Organisasi Pemerintah.* Penyempurnaan Makalah pada Workshop Manajemen Perkantoran di Lingkungan Kementerian Komunikasi dan Informatika. Bandung.

[7] Lexy. J. Moleong., Metodologi Penelitian Kualitatif, (Bandung: PT Remaja Rosdakarya, 2000).

[8] Peltier, T. R., 2001, Information Security Risk Analysis, Auerbach Publications.

[9] Repo.unair.ac.id/data/kompetensi/usi/risk%20Assessment.pptx., 20 januari 2015.

[10] Standar Nasional Indonesia, SNI ISO/IEC 27001:2009, Teknologi Informasi – Teknik Keamanan – Sistem Manajemen Keamanan Informasi – Persyaratan

[11] Sarno, R. dan Iffano, I. 2009. Sistem Manajemen Keamanan Informasi. Surabaya: ITS Press.

[12] Tim direktorat keamanan informasi, "Panduan Penerapan Tata Kelola Keamanan Informasi Balai Pelayanan Publik" Edisi: 2.0,September 2011, Kementrian komunikasi dan informatika RI.